Subject: KWIC Security

Effective Date: September 1, 2017 Revised from: October 1, 2015

Policy: Individuals, including WIC staff and State Agency employees, involved in the WIC certification and benefit issuance process, are responsible for the safeguarding of WIC Program client information and the physical equipment used in the administration of the program.

Procedure:
WIC clinic IT support staff and other appropriate staff must follow the measures outlined below regarding physical, network, and operating system levels of security.

Layer	Security Practices Required
Operating System	• Apply latest service packs and security patches in a timely manner. • Disable all unnecessary services. • Enable strong password policies at the Local Agency level. • Install and automatically update anti-virus protection.

Clinic Specific Items

1. Physical Site

Local Agencies are required to exercise physical security of KWIC equipment, data and supplies. Buildings containing WIC equipment should be locked and secured outside of regular business hours.

2. Virus Protection

All workstations used for KWIC must have up-to-date virus protection software installed. The software must be configured to automatically update itself on a regular basis.

Users are required to follow established policies prohibiting downloading and/or installing unauthorized applications or data onto WIC computers. Staff should comply with KDHE and local agency policies regarding downloading approved applications and virus screening.

3. Network Security

WIC staff must enter an account name and password to gain access to the Local Area Network (LAN) at the clinic. LAN user accounts and access privileges will be managed locally. Clinics that have existing networks and local IT support are responsible for managing their own local network security.